Paul Connelly
Hospital Corporation of America

HIT Standards Committee

Hearing on Health Information Technology Security Issues, Challenges, Threats, and Solutions

Systems Stability and Reliability Panel

November 19, 2009

Questions:

1. Briefly describe your organization and your information security approach to system stability and reliability.

Hospital Corporation of America, also known as HCA, is a privately-owned company that operates 163 hospitals, 112 freestanding outpatient centers, and dozens of other types of company facilities and support organizations in twenty states and England. HCA's Information Technology and Services organization supports all HCA hospitals and facilities and also provides outsourced IT support to more than 100 other non-HCA hospitals. We have 183,000 employees and support more than 60,000 independent physicians who work in HCA facilities.

Our hospitals in many geographic areas are organized into markets that share patients, physicians, and patient data—in effect, our own "mini-HIE." Our hospitals and facilities use common IT and clinical systems connected to a company-wide data network run out of five hub data centers. In addition, many clinical and IT systems are locally based in our hospitals, and connected to the company data network. Our IT systems are utilized in virtually all areas of our patient care and operations.

Information Security plays a key role in stability and reliability of our systems. We have an 85-person security team that does everything from policy to implementation, to operation of key infrastructure pieces, to follow-up assessment and tracking of remediation. Our security team partners with our Clinical Services Group and other business units to identify and build security measures into every system and our network, and bake secure practices into our processes wherever possible, to ensure the integrity of the data and the availability of the systems. We actively monitor the systems and network around the clock for both performance and for security vulnerabilities and attacks. We also train and regularly remind our users about security practices and the need to protect data and systems.

Quality patient care depends on the integrity of the data in our systems as well as the availability of these systems, making system stability and reliability vital to us. There is no silver bullet—failover, redundancy, and security are built into each layer of our systems and the network. Our approach includes:

- Having well-defined security policies and standards
- Deploying consistent and hardened system configurations

- Keeping the systems current with timely patching and upgrades
- Having a comprehensive security program that proactively looks for vulnerabilities and threats
  - e.g., we conduct monthly scans of the 375,000+ devices on our network to identify vulnerabilities and assign remediation tasks
- Deploying security tools like Anti-Virus and keeping them up-to-date
- Maintaining strong perimeter network filtering and firewalls, wireless controls, and remote access controls
- Strongly authenticating users requesting access to our systems
- Identifying and responding quickly to risk and incidents.
  - A key part of our approach is to maintain a Security Event Management (SEM) system that correlates data from server logs, firewalls, Intrusion Detection System nodes, Anti-Virus systems, and other sources to provide near real-time information to pinpoint and assess risks on our network

2. Provide one or two examples of information security issues you have faced recently related to system stability and reliability, and describe how you addressed these issues.

Technical Security Threats. Early this year we had to battle infections of devices on our network by the "Conficker" worm. Despite almost immediate detection and response, this worm was able to infect more than 1700 hosts on the HCA network before we could contain it.

- Our regular vulnerability scans identified systems that were vulnerable to this worm
- Our network monitoring systems were able to identify the activities of Conficker-infected systems in near real-time, and identify them as malicious and characteristic of a worm
- We used routing and other techniques to quarantine the infected devices to stop the propagation
- We went into incident response mode and our data center and facility IT teams executed system cleanup routines

This is a good example of a problem I hope we can discuss today—the security of FDA certified or vendor-managed clinical systems. Of the 1700 devices on our network that were infected by Conficker, exactly ONE was a device managed by HCA's IT team; the 1699 other devices were vendor systems—where we are dependent on the manufactures to provide for patching, anti-virus, and other basic security measures. As Conficker demonstrated, many Vendors are not meeting the need. This includes pharmacy and clinical systems where data integrity and system availability can be critical.

We feel we do a good job managing the security of our network, but our hands are tied on many of these vendor systems. They compromise about 10% of the devices on our network and are one of the biggest risks we face to security and therefore stability and reliability.

Natural threats. Many HCA hospitals are in geographical areas susceptible to hurricanes, and several of our facilities along the Gulf Coast were significantly impacted by Hurricane Katrina. As these hospitals put rehearsed contingency plans into action, our IT organization likewise transitioned to back-up communications, data systems and data centers. Key lessons learned include –

- Our contingency plans have had to move beyond just Disaster Recovery of IT systems to focus more on continuity of operations-- with more emphasis on electrical power, voice communication, and data communication.
- There must always be a way for a caregiver to "break the glass" if necessary to provide critical care. Breaking the glass, however, must be audited and subject to post-incident review and validation.
    - e.g., we had to adjust our normal standards to enable urgent patient care by volunteer physicians, nurses, and other clinicians who did not have user credentials on our systems.

3. What kinds of trade-offs have you had to make between security and usability, and other operational considerations?

Balancing ease-of-use with security needs is a daily challenge in the health care provider space. Clinical users such as physicians often move around a hospital or between hospitals, and any security measures that slow or complicate their access could impact patient care.

As part of our diligence to comply with industry standards and regulations, we have gone to great lengths to determine what approaches are reasonable for our clinicians. The key areas of our focus have been on:

- Reducing the number of IDs and passwords users require through integration with our Active Directory infrastructure, implementation of a Single Sign On product, and implementation of Identity Federation where feasible.
- Reducing the number of logons through the above actions, managing session and screen-saver time-outs, and implementing patient-context-aware application logons and session retention capabilities.
- Increasing the speed of logons through the use of badge RFIDs for logon in place of manually-entered IDs and passwords
- Automating user account request, approval, and set-up to reduce lost time through the establishment of roles-based access and automated user provisioning
- Increasing the ease of remote access to our systems.
    - e.g., our current conversion from a token-based authentication for remote users to an Adaptive Authentication approach that saves the user time and reduces complexity, while maintaining two-factor authentication.

      Within months of implementing this remote access approach we received feedback from two different physicians who told us they believed the time saved by our new system made the difference in the outcome for their patients.

When we have made trade-offs, they have been risk based and most-often made for systems in care areas (e.g. ERs, treatment rooms, etc) where compensating controls mitigate the risk.

4. What information security standards are you currently using to meet your business needs for system stability and reliability?

HCA uses an internally-developed framework of policies, standards, guidelines, and operational procedures based on several industry standards and practices, including:

- HIPAA Security Rule
- ISO 17799
- NIST 800-30
- Payment Card Industry Data Security Standards
- Industry best practices for system back-up, continuity of operations, and disaster recovery.

HCA has been a participant since the start up of an industry organization called HITRUST, which has been working over the past two years to develop health care industry-wide collaboration and agreement on a common security framework and other tools. HITRUST has gained the involvement and support of a broad section of the health care industry, has published a Common Security Framework, and is also facilitating industry-wide cooperation and collaboration to address key security issues. I recommend the committee look at HITRUST's activities to see how their efforts can fold into yours to save time and avoid duplication of effort.

5. What challenges have you had to address in implementing these standards (e.g., training)?

There are three key aspects of this challenge:

Internally:

- Simply getting guidance out to all corners of our enterprise is the first step and is a challenge. Reaching the Holy Grail of getting the guidance out, having the right people understand the direction, and having the direction followed requires relentless communication, tying the guidelines to specific situations and systems with step-by-step operational procedures, following up with checks and audits, and tracking follow-up to the follow-up.
- The lack of support for basic security controls on vendor systems may be our biggest challenge in implementing security standards. As our Conficker worm experience demonstrated, we do a fairly good job managing our own systems, but the vendor systems we don't manage are a huge risk. These are not "Mom and Pop" vendors or older devices--some of the biggest manufacturers of clinical systems in the country sell devices to our hospitals *today* that are not built with basic security and identity management capabilities. Implementation of our standards on these systems is a huge

challenge, and they pose of significant risk to the security, stability, and reliability of our network and data.

Many vendors use FDA certification as their justification for making their systems untouchable. If we are going to have secure, stable, and reliable EHRs and HIEs, the Vendors of clinical systems have to bake security into their products, and the FDA certification should enable these features, not be used as an obstacle.

Externally:

- One of our biggest challenges has been the variation in interpretation of guidelines like the HIPAA security rule. We constantly hear that we have an overly-strict interpretation of the security rules, and the other hospitals that are our neighbors to ours don't require the same levels of security. In some cases this actually puts us at a competitive advantage, as "security and reliability" have not proven to be physician attractors.

6. What is the role/value of interoperable information security standards in helping assure system stability and reliability?

Consistent standards are essential, especially as systems and users exchange patient information across different systems and networks.

- Clinical systems and hospitals are quite diverse--the industry must have a consistent approach to exchange EHRs and other patient information.
- Speed of access, integrity of data, identification of users, redundancy, and availability of systems all depend on a consistent implementation of standards.

The HIPAA Security Rule allowed a substantial amount of interpretation and self-determination of how it would be implemented. As a result, today there are hospitals right across the street from one-another that have substantially-different security measures in place. If those hospitals are to have enough confidence in one-another's ability to protect sensitive patient data that they will someday exchange health information, there has to be very specific interoperable security standards.

7. What are the current limitations or gaps in interoperable information security standards with respect to system stability and reliability?

Not only is there wide variation in systems and data forms between providers, as stated above in #6, many standards are open to interpretation, and those interpretations can vary widely from organization to organization.

Systems might work well within a single organization, but not be set up to facilitate stable and reliable exchange of information of information across organizations. Vendors actually have financial incentive today to create proprietary systems, because proprietary systems bring more work and revenue to them. Unless that model is broken through standards of interoperability, it will be extremely complex and expensive to attain.

Stability and reliability are also likely to vary widely in cases of technical (e.g., a major worm outbreak) or natural (e.g., hurricane) disasters.

Well-defined standards are needed, and need to include the requirements for information exchange, e.g., encryption, federation of authentication and authorization.

8. What new and emerging issues around system stability and reliability do you foresee over the next 2-3 years?

- **Data exchange** will be a big challenge to stability and reliability. As clinical systems connect more and exchange more information, the risk from systems that are susceptible to vulnerabilities, threats, and outages spreads to other systems-- the risk of the whole "ecosystem" is tied to the lowest common denominator. For this reason, there has to be some type of assurance program to validate the controls of each organization plugging into regional and national networks. This program must scale from large national organizations to physician practices.
- **External hosting of systems via ASP/Cloud Computing**— Economic conditions and ARRA stimulus around HIT adoption is likely to drive more organizations to use technologies that are managed and supported by third parties. This presents a new level of exposure to organizations, as these vendors become critical to the stability and reliability of the system.

  Where is our data? Who has access to it? Who legally owns it? How do I get to it in an outage? How reliable are all the components of the connection? These are all questions that can be difficult to answer with Cloud-based solutions.

  Providers need to be able to effectively assess the ability of these companies to protect our data, and have a way of ensuring ongoing compliance with requirements. Some type of universally-shared attestation and ongoing review would facilitate this process and prevent each provider from independently conducting.

  (The idea of an assurance program for entities that "plug into" and HIE and a shared assessment of 3rd parties are both areas of focus of the HITRUST organization that merit review by the committee)
- **"Fraud as a Service"-** the growing organization of the cybercrime "business" and targeting of health care as a source of financial gain places a layer of urgency over the security of EHRs and HIEs.
- **Mobility**—growth in the use of mobile devices, as well as the mobile and work-from-home workforce means data will be on more diverse systems that are not always controlled by the HC organizations
- **Use of Social Media**—there are numerous examples of how social media can be used to improve effectiveness of health care operations and patient care, however, it also creates risk.